Les modes alternatifs de régulation

Poullet, Yves

Published in:
Le règlement général sur la protection des données (RGPD/GDPR)

Publication date:
2018

Document Version
le PDF de l'éditeur

TITRE 7
Les modes alternatifs de régulation : codes de conduite, certifications et ADR dans le RGPD

Yves POULLET[1]

1. Le règlement général sur la protection des données (« RGPD »)[2] se caractérise non tant par l'innovation de son contenu que par sa volonté de rendre effectifs les principes de protection des données. Cette volonté est traduite en premier lieu, par l'approche techno-légale adoptée : *privacy by design, privacy by default, privacy impact assessment*, par l'utilisation par les personnes concernées des technologies dans l'exercice de leurs droits ; en deuxième lieu, par l'extension des compétences des autorités de protection des données en particulier par la mise à disposition de ces autorités du pouvoir de sanctionner administrativement les infractions au Règlement, et en troisième lieu, par la possibilité de recours collectifs des personnes concernées. Sans doute, est-ce là également l'explication de l'importance accordée aux modes de régulation alternatifs.

Parce que conçus par les acteurs du marché eux-mêmes, si possible après concertation ou consultation des associations représentant les personnes concernées[3], ces instruments sont plus en lien avec la réalité et les spécificités des opérations en cause. Leur contenu constitue, dès lors, une traduction adaptée au secteur d'activités des dispositions du Règlement qui, souvent générales, sont susceptibles d'interprétations variées et d'applications différenciées suivant le type d'opérations. Par ailleurs, ces instruments proposent, d'une part, des mécanismes de contrôle et, d'autre part, des solutions en cas de litiges et de sanctions plus rapides, efficaces et adéquates que les sanctions administratives et judiciaires proposées par l'ordre juridique traditionnel. Enfin, parce que

[1] Professeur émérite à la faculté de droit de l'UNamur, Professeur associé à l'Université catholique de Lille, Membre de l'académie royale de Belgique.

[2] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

[3] L'article 16 de la directive e-commerce de 2002 préconise cette co-rédaction des codes de conduite dans les transactions électronique B to C.

discutés et acceptés par le secteur, ils jouissent d'une légitimité forte auprès des acteurs concernés[4].

2. Tout cela est à souligner et on ne s'étonne dès lors pas que leur promotion soit particulièrement encouragée[5]. La section 5 du chapitre IV intitulé « Responsable du traitement et sous-traitant » leur consacre cinq longs articles (art. 40 à 44). On note la référence du règlement aux besoins particuliers des petites et moyennes entreprises qui trouveraient dans ces mécanismes une façon aisée de satisfaire aux prescrits réglementaires. Il est vrai que les codes de conduite constituent une solution mutualisée adéquate pour des entreprises qui ne peuvent se permettre d'investir la matière de la protection des données et définir elles-mêmes leur politique en la matière[6].

Sous l'empire de la directive 95/46/CE, un seul article, l'article 27, avait ouvert la voie à la reconnaissance de ces instruments, en mentionnant la possibilité pour les entreprises de se référer à des codes de conduite, et incitait ces dernières à développer ces codes au niveau européen et à les faire agréer par les autorités de protection des données voire au niveau européen par le Groupe de l'article 29. Cette entrée timide des modes alternatifs de régulation en 1995[7] fait place, 20 ans après, à une affirmation plus large de l'intérêt de ces mécanismes sans pour autant déboucher, loin s'en faut, sur le système américain qui prône une solution principalement auto-régulatrice de la protection des données[8]. En effet, le système européen s'il admet

---

[4] Même s'il faut le reconnaître, ce sentiment de légitimité peut varier en fonction de différents facteurs. Ainsi, la légitimité sera plus forte si le code est conçu avec les organisations et entités concernées et non imposé par le secteur.

[5] « Les États membres, les autorités de contrôle, le comité et la Commission encouragent l'élaboration de codes de conduite destinés à contribuer à la bonne application du présent règlement, compte tenu de la spécificité des différents secteurs de traitement et des besoins spécifiques des micro, petites et moyennes entreprises » (art. 40. 1 du RGPD). Même encouragement à propos de la certification et des labels à l'article 42.1.

[6] Notons que ces entreprises sont dispensées de la nomination d'un délégué à la protection des données imposée aux grosses entreprises et dont le rôle est précisément d'aider en interne l'entreprise à définir sa politique en matière de protection des données et les moyens de sa réalisation (sur cette fonction et ses missions, lire les articles 38 et 39 du règlement et leurs commentaires dans le présent ouvrage).

[7] Voy. par exemple sur la base de l'article 27, les codes de conduite européens de la FEDMA (Marketing direct, 2010) et du Cloud Select Industry Group (Cloud computing, 2015) ayant fait l'objet d'avis du Groupe 29.

[8] De manière critique sur la solution de l'auto-régulation en matière de vie privée aux États Unis, lire R. Gellman et P. Dixon, « Failures of Privacy Self-regulation in the United States », in *Enforcing Data Protection* (D. Wright et P. De Hert eds), Springer, 2016, pp. 53 et s. ; *cf.* égal. l'étude très fouillée et comparative de nombreuses *Privacy Policies* et de leurs ambiguïtés, J. Reidenberg, J. Bhatia, T. Breaux et T. Norton, « Ambiguity in Privacy Policies and the Impact of Regulation », *Journal of legal Studies,* 2016, vol. 43, pp. 163 et s.

des méthodes alternatives de régulation en subordonne la légitimité à une stricte conformité à la loi et ne les envisage en définitive que comme moyen de lui ajouter des précisions et bien évidemment une effectivité renforcée.

3. Notre propos sera donc triple. Dans un premier temps, nous examinerons les différents instruments de régulation alternatifs proposés par le Règlement dans l'ordre interne européen : les codes de conduite, la certification en ce compris les labels. Dans un deuxième temps, nous verrons les multiples balises mises à la reconnaissance de ces instruments qui permettent de distinguer l'approche auto-régulatrice américaine et celle de co-régulation proposée par l'Union Européenne. Dans un troisième temps, nous analyserons la reconnaissance de ces instruments dans le cadre des flux transfrontières et ce à la lumière des dispositions du « *Privacy Shield* » qui a remplacé la décision de la Commission de 2000 relative aux flux EU/US dite « *Safe Harbor Principles* » et de celles relatives aux « règles d'entreprises contraignantes » (*Binding Corporate Rules*) prises par les groupes d'entreprise pour satisfaire aux exigences d'adéquation du règlement en cas de flux transfrontières.

CHAPITRE 1. Les mécanismes de régulation alternatifs : code de conduite, certification et modes alternatifs de règlements des litiges (les ADR)

4. Là où la défunte directive 95/46 se contentait d'évoquer les seuls codes de conduite différents types de mécanismes d''auto-régulation' sont promus par le Règlement : les codes de conduite (art. 40), la certification (art. 42), en ce compris les labels, et les « procédures extrajudiciaires et autres procédures de règlement des litiges » que le Règlement invoque incidemment[9]. Par ailleurs, le Règlement prend soin de préciser l'étendue de leur objet possible depuis le traitement loyal jusqu'à la notification

[9] On retrouve la référence aux modes alternatifs de règlement de litiges dans l'énumération des objets des codes de conduite (art. 40.2) au point k) : « les procédures extrajudiciaires et autres procédures de règlement des litiges permettant de résoudre les litiges entre les responsables du traitement et les personnes concernées en ce qui concerne le traitement, sans préjudice des droits des personnes concernées au titre des articles 77 et 79 ».

aux autorités de contrôle[10]. Revenons sur chacun de ces mécanismes et analysons leurs effets dans le Règlement.

SECTION 1. – Les codes de conduite

5. Le code de conduite parfois également dénommé charte ou code déontologique (en anglais, le plus souvent Code of Conduct ou Company's Policy) constitue une déclaration officielle de valeurs éthiques ou de bonnes pratiques qui seront tenues par rapport à des tiers internes à l'entreprise, l'association ou l'administration comme les employés et les chercheurs, ou externes, qu'ils s'agissent de fournisseurs, de clients ou de pairs (exemple : un code sur la concurrence loyale). Le code formalise un certain nombre de principes d'actions et de normes « minimales ». En adoptant et publiant son code de conduite, l'entreprise s'engage à observer ces normes et à les faire observer par ses sous-traitants et fournisseurs. Il peut être propre à une entreprise, une association ou, au contraire, se nouer dans le cadre d'ententes entre certaines entreprises voire d'associations sectorielles. Le code concerne souvent une activité plus ou moins spécifique et un thème particulier. La préoccupation des rédacteurs des codes est double : il s'agit, auprès des destinataires du code de donner

[10] Ainsi, l'article 40 suggère l'existence de codes de conduite dans les matières suivantes :
« a) le traitement loyal et transparent ;
b) les intérêts légitimes poursuivis par les responsables du traitement dans des contextes spécifiques ;
c) la collecte des données à caractère personnel ;
d) la pseudonymisation des données à caractère personnel ;
e) les informations communiquées au public et aux personnes concernées ;
f) l'exercice des droits des personnes concernées ;
g) les informations communiquées aux enfants et la protection dont bénéficient les enfants et la manière d'obtenir le consentement des titulaires de la responsabilité parentale à l'égard de l'enfant ;
h) les mesures et les procédures visées aux articles 24 et 25 et les mesures visant à assurer la sécurité du traitement visées à l'article 32 ;
i) la notification aux autorités de contrôle des violations de données à caractère personnel et la communication de ces violations aux personnes concernées ;
j) le transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales ; ou
k) les procédures extrajudiciaires et autres procédures de règlement des litiges permettant de résoudre les litiges entre les responsables du traitement et les personnes concernées en ce qui concerne le traitement, sans préjudice des droits des personnes concernées au titre des articles 77 et 79 ».

une image positive de l'entreprise et, souvent, dans le même temps de se démarquer des concurrents[11].

Les codes de conduite en matière de protection des données à caractère personnel (les « *Privacy Policy* ») et souvent de sécurité des données n'échappent pas à la règle. À côté des codes propres à une entreprise[12] ou à un groupe d'entreprises[13], on trouve des codes souscrits par des secteurs entiers[14], comme le secteur de la publicité, celui des distributeurs, etc. Aux codes propres à une activité[15], s'ajoutent des codes relatifs à l'entreprise comme telle. La multiplication de tels codes s'explique d'abord par la nécessité pour les personnes concernées de connaître leurs interlocuteurs dans des marchés devenus, grâce à l'Internet, globaux et non plus marqués par une proximité qui permettait de connaître facilement la politique menée par ces derniers. Ensuite, ce mouvement né aux États-Unis se comprend par la volonté des entreprises de répondre au principe *d'accountability* mis en évidence par l'OCDE que l'on peut résumer comme suit : « *Tell me what you are doing and do it effectively* ». Le *False and Deceiptive Statement Act,* loi votée aux États Unis en 1970 permet de sanctionner les déclarations qui ne correspondent pas à la réalité ou induisent le consommateur en erreur et charge la *Federal Trade Commission* de poursuivre de telles infractions. Son bilan, même s'il est limité[16] et n'est pas exempt d'ombres[17], mérite d'être souligné[18].

---

[11] M. Wurgler, « Self-Regulation and Competition in Privacy Policies », *Journal of Legal Studies,* 2016, vol. 45, pp. 13 et s.

[12] Ainsi, des entreprises comme DAIMLER (*www.mercedesbenz.ma/.../CodeOfConduct.../Code_of_Conduct_franz_2007.pdf),* PROXIMUS (https://www.proximus.com/sites/default/files/.../proximus_code_of_conduct_fr.pdf) ; Société Générale de Banque (*https://www.privatebanking.societegenerale.be/.../Code_de_Conduite_SG.pdf*).

[13] Nous reviendrons plus loin (*infra*, n° 20) sur les règles d'entreprises contraignantes signées par des multinationales.

[14] Ainsi, dans le secteur financier belge, le code FEBELFIN (www.bonnerelationbancaire.be).

[15] À ce propos, le code SECUREX à propos de l'utilisation des réseaux sociaux par les employés et la protection de leur vie privée (www.securex.eu/lex-go.nsf/PrintReferences?OpenAgent&Cat2=49~~10&Lang).

[16] La FTC est compétente dans les matières touchant la consommation à l'exception de certains secteurs d'activités (la banque, l'assurance, le transport et les télécommunications), elle ne l'est point en matière d'emploi, ou d'activités non commerciales.

[17] Nous reviendrons *infra*, n^{os} 6 et 22 sur les critiques adressées par certains auteurs américains et par le Groupe 29 à l'action de la FTC.

[18] Sur le travail de la FTC en matière de protection et de sécurité des données et les nombreux exemples y cités, lire l'US FTC Commissaire J. Brill, « Privacy and Data Security in the Age of Big Data and the Internet of Things », discours tenu au Washington Governor Jay Inslee's Cyber Security and Privacy Summit, le 5 janvier 2016, disponible sur le site https://www.ftc.gov/system/files/documents/public_statements/904973/160107wagovprivacysummit.pdf : « *Eighty years ago, Congress gave the FTC authority to protect consumers from a broad range of "unfair or deceptive acts or practices." Under this authority,*

Ces codes sont généralement structurés[19] en suivant les principes retenus tant par l'OCDE que par le Conseil de l'Europe[20]. Ils peuvent faire référence à des mécanismes de négociation, de révision, de publicité tant interne qu'externe, de contrôle du respect et de possibilité pour les destinataires d'adresser toute plainte, remarque ou critique à l'égard du texte du code comme de son respect. Ils peuvent ainsi nommer une personne de contact et reprendre en annexe un formulaire *ad hoc*. Enfin, des mécanismes de certification, des labels et des mécanismes de résolution des litiges (voy. points B. et C.) peuvent être attachés à l'existence d'un code et garantir son respect.

---

the FTC has brought nearly 100 privacy and data security enforcement actions. The flexibility and breadth of our authority to obtain remedies that protect consumers has allowed us to keep up with rapid changes in technology. For example, we have brought actions against companies for allegedly collecting information inappropriately from consumers' mobile devices, making unwarranted intrusions into private spaces, exposing health and other sensitive information, exposing previously confidential information about individuals' networks of friends and acquaintances, and providing sensitive information to third parties who in turn victimize consumers ».

[19] Voy. à cet égard le logiciel mis au point par diverses universités américaines (Carnegie Mellon, Fordham, Stanford) : The Usable Privacy Policy Project, Towards Effective Web Privacy Notice and Choice (http://usableprivacy.org) qui permet d'appréhender la structure de chaque « *privacy policy* ».

[20] Ainsi, le règlement (article 40) liste les rubriques suivantes : « - le traitement loyal et transparent ;

- les intérêts légitimes poursuivis par les responsables du traitement dans des contextes spécifiques ;
- la collecte des données à caractère personnel ;
- la pseudonymisation des données à caractère personnel ;
- les informations communiquées au public et aux personnes concernées ;
- les modalités d'exercice des droits des personnes concernées ;
- les informations communiquées aux enfants et la protection dont bénéficient les enfants et la manière d'obtenir le consentement des titulaires de la responsabilité parentale à l'égard de l'enfant ;
- les mesures techniques et organisationnelles, ainsi que les procédures visées au RGPD devant être déployées pour le respect des principes d'*accountability*, *de privacy by design* et de *privacy by default*, ainsi que les mesures visant à assurer la sécurité du traitement ;
- la notification aux autorités de contrôle des violations de données à caractère personnel et la communication de ces violations aux personnes concernées ;
- le transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales ;

ou

- les procédures extrajudiciaires et autres procédures de règlement des litiges permettant de résoudre les litiges entre les responsables du traitement et les personnes concernées en ce qui concerne le traitement ».

6. La doctrine[21] attire l'attention sur le langage utilisé par les codes de conduite, en particulier, sur le flou voire l'ambiguïté des termes utilisés par nombre de codes de conduite[22]. Cette ambiguïté est destructrice de la confiance que les lecteurs de tels codes peuvent mettre dans la qualité de l'engagement.

Enfin, nous signalons le fameux projet P3P (*Platform for Privacy Preferences)* à l'initiative du consortium W3C mis au point par ATT et adopté (puis abandonné) par Microsoft[23]. Ce projet visait à standardiser le moyen par lequel un site web peut informer l'internaute de sa politique en matière de protection des données personnelles. La plateforme P3P, intégrée dans le navigateur de l'internaute, avait pour ambition, à partir de certains mots clé, de permettre à ce dernier de sélectionner ses préférences en matière de respect de ses données à caractère personnel (exemple : pas de transfert à des tiers de mes données à caractère personnel, pas de données sensibles, durée de conservation limitée à X années, …) et garantissait par une analyse sémantique des '*privacy policies'* des entreprises présentes sur le web de bloquer (avec négociation possible) l'accès aux sites web ne respectant pas ces préférences exprimées.

SECTION 2. – Les certifications et labels

7. Les mécanismes de certification, de normes techniques et de labels[24] sont prévus aux articles 42 et 43 du RGPD. Ces mécanismes ont vocation

[21] J. R. Reidenberg, J. Bhatia, T.D. Breaux, and T.B. Norton, « Ambiguity in Privacy Policies and the Impact of Regulation », *Journal of Legal Studies*, 2016, vol. 45, pp. 163 et s. ; J. Bhatia, T. D. Breaux, J. R. Reidenberg and T. B. Norton, « A Theory of Vagueness and Privacy Risk Perception », *Paper presented at the Institute of Electrical and Electronics Engineers 24th International Requirements Engineering Conference*, Beijing, September 2017, 12-16 et les références y citées.

[22] Ainsi dans l'article cité de Reidenberg *et alii*, leurs conclusions : « *From the inter- and intra-category vagueness results, we theorize that differences in clarity may be due to one of three semantic functions : likelihood, which is the possibility that something is true ; authority, which is whether an action is discretionary or mandatory ; and certitude, which is the absoluteness with which something is true. For example, "likely" is more clear than "possibly," both of which concern the degree or likelihood that a data practice occurs. Authority refers to whether the practice is permitted, required or prohibited, and it may be true that required practices are perceived as more clear than permitted practices : "as needed" is perceived as more clear than "as appropriate." Similarly, the vague term "may" denotes both permissibility and possibility, and is perceived to be more clear than "can," which denotes capability and not necessarily authority* ».

[23] Le Groupe 29 a émis un avis sur ce projet ; *ec.europa.eu/justice/policies/privacy/docs/wpdocs/1999/wp16fr.pdf.*

[24] Sur l'effectivité des certifications et labels, lire K. Block, « Data Protection Certification : decorative or effective Instrument ? Audit and seals as a Way to Enforce Privacy », in *Enforcing Data Protection* (D. Wright et P. De Hert eds), Springer, 2016, p. 335. La question

en particulier à être des outils qui permettront de « démontrer que les opérations de traitement effectuées par les responsables du traitement et les sous-traitants respectent le […] règlement »[25]. Ces mécanismes, dit le règlement, devront être **volontaires et accessibles via un processus transparent**. Nous ajouterions volontiers qu'ils doivent être ouverts sans discrimination.

Ils sont souvent liés à un code de conduite dont le mécanisme de certification et l'attribution d'un label ont pour but de vérifier le respect et d'attester ce dernier. On distinguera différents types de certifications[26] : celles menées par des autorités publiques, celles, par des autorités privées ; celles spécifiques au respect de la législation 'Protection des données' et celles, plus larges, envisageant l'ensemble des questions liées au commerce électronique, comme la qualité du service, le respect des prescrits de protection des consommateurs, d'archivage des transactions, etc. ; celles fondées sur une auto-certification avec la possibilité de contrôle *a posteriori,* celles au contraire fondées sur une certification préalable[27]. La question du coût de la certification doit également être soulignée, comme celle de

---

de la responsabilité des organismes de certification et de labellisation a été étudiée par P. Balboni (« Model for an Adequate Liability System for Trustmark Organisations », in S. M. Kerkegaard (ed.), *Legal, Privacy, and Security Issues in Information Technology*, vol. 1, *The First International Conference on Legal*, Privacy and Security Issues in IT Hamburg, Germany, April 30 - May 2, 2006 *Proceedings COMPLEX 3/06*, Institutt for rettsinformatikk, Oslo, pp. 97-111).

[25] À cet égard, lire L. Landes- Gronowskt, « Le RGPD en focus -Précisions sectorielles et métiers sur les implications du RGPD », *Focus 3*, avril 2017, disponible à l'adresse suivante : http://www.avistem.com/sites/default/files/2017%2004%2003%20Article%20RGPD%20focus%20codes%20de%20conduite%20labels%20certifications%20V.....pdf., qui établit la liste des normes existantes et à venir, mais également de manière plus large des outils qui peuvent et pourront être utilisés par les responsables de traitements et sous-traitants dans le cadre de leur mise et de leur maintien en conformité aux obligations qui leur incombent en matière de protection des données à caractère personnel.

[26] C. Connolly, « Benchmarks for Global Privacy Strandards », *Working Paper*, novembre 2009, Pyrmont. On distinguera les labels et certificats américains comme Trust-e (http://www.etrust.org/) : « *A PrivacyTrust Certification indicates that your website has been reviewed by PrivacyTrust and has met our stringent privacy and data protection requirements. Having a PrivacyTrust Seal on your website signifies to customers that any critical data collected, such as home addresses and phone numbers are not exchanged with third parties without their consent. This is vital in having a trustful relationship between you and your customers* » ; (www.bbonline.com) ; Webtrust (www.webtrust.org/) ; ou européens comme EURO PRISE (https://www.european-privacy-seal.eu/.../5e13d520-1af0-4af0-a5a.) ; *e-PRIVACY* (https://www.eprivacy.eu/fr/labels-de-protection) ou *TRUSTED SHOPS* (www.trustedshops.be/fr/label-de-qualite/protection-acheteur.html) moins centrés sur la question de la protection des données à caractère personnel.

[27] A. Rossnagel, « Datenschutz-Audit », *DuD*, 2007, pp. 565 et s.

la périodicité dans la mesure où le contrôle porte sur la situation à un moment donné[28].

Les sanctions liées aux systèmes de certification et de labellisation varient : tantôt, l'infraction aux règles amène le retrait du label sans plus, tantôt s'ajoute une amende et/ou, surtout, la publicité via une *blacklist* de la décision motivée. Les promoteurs de ces certifications sont généralement des associations privées travaillant dans un marché concurrentiel, ce qui, selon certains auteurs risquent de les mettre dans une position délicate lorsqu'il s'agit de 'sanctionner' un client.

8. Enfin, on notera l'intérêt du recours pour les entreprises à ces modes de régulation. Certaines dispositions du Règlement prévoient que les responsables ou sous-traitants peuvent justifier de leur conformité aux exigences du RGPD en exhibant du suivi d'un code de conduite ou d'une certification[29]. Le § 3 de l'article 4 ajoute que l'application de mécanismes d'autorégulation accrédités constitue un « élément », voire une présomption *iuris tantum*, de démonstration du respect des obligations de moyen mis à sa charge.

On retient également la possibilité pour la Commission, selon l'article 40.9, de « décider, par voie d'actes d'exécution, que le code de conduite, la modification ou la prorogation approuvés qui lui ont été soumis en vertu du paragraphe 8 du présent article sont d'application générale au sein de l'Union ». Cette prérogative de la Commission est répétée, à l'article 43.9, à propos des procédures de certification ou de labellisation. Par voie d'actes d'exécution, le Règlement, en son article 92, entend permettre l'exercice par la Commission de délégations soumises à un contrôle parlementaire[30].

---

[28] Nous nous référons à l'étude complète réalisée par le CRIDS pour l'Union européenne : F. DE VILLENFAGNE, F. DUMORTIER et Y. POULLET, *Comparison of Privacy and Trust Policies in the Area of Electronic Communications : final report*, 2007, Namur, Facultés Universitaires Notre-Dame de la Paix : http://www.crid.be/pdf/public/5596.pdf ; O. TAMBOU, « L'introduction de la certification dans le règlement général de protection des données à caractère personnel : Quelle valeur ajoutée ? », *RLDI,* 2016/126, n° 3986, pp. 43 et s.

[29] Ainsi en matière de sécurité, l'article 32, § 3, dispose : « L'application d'un code de conduite approuvé comme le prévoit l'article 40 ou d'un mécanisme de certification approuvé comme le prévoit l'article 42 peut servir d'élément pour démontrer le respect des exigences prévues au paragraphe 1 du présent article ».

[30] L'article 92, § 5, précise : « Un acte délégué adopté en vertu de l'article 12, paragraphe 8, et de l'article 43, paragraphe 8, n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de trois mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de trois mois à l'initiative du Parlement européen ou du Conseil ».

9. Par ailleurs, outre leur application par les responsables de traitements ou les sous-traitants soumis au RGPD, les codes de conduite qui seront approuvés et d'application générale pourront aussi être appliqués par des responsables de traitements ou des sous-traitants qui ne sont pas soumis au RGPD, afin de fournir des garanties appropriées dans le cadre de transferts de données à caractère personnel vers un pays tiers ou une organisation internationale par exemple. Ces responsables de traitements ou sous-traitants devront alors à cette fin prendre l'engagement contraignant et doté de force obligatoire, au moyen d'instruments contractuels ou d'autres instruments juridiquement contraignants, d'appliquer ces garanties appropriées, y compris en ce qui concerne les droits des personnes concernées.

Outre leur application par les responsables de traitements ou les sous-traitants soumis au RGPD, les mécanismes de certification ou les labels approuvés en matière de protection des données pourront être établis aux fins de démontrer que des responsables de traitements ou des sous-traitants qui ne sont pas soumis au RGPD fournissent des garanties appropriées dans le cadre de transferts de données à caractère personnel vers un pays tiers ou une organisation internationale par exemple. Ces responsables de traitements ou sous-traitants devront à cette fin prendre l'engagement contraignant et exécutoire, au moyen d'instruments contractuels ou d'autres instruments juridiquement contraignants, d'appliquer ces garanties appropriées, y compris en ce qui concerne les droits des personnes concernées.

SECTION 3. – Les mécanismes de règlement des litiges : les ADR et ODR

10. Le règlement évoque la possibilité pour un code de conduite de renvoyer à une procédure extrajudiciaires de règlement des litiges. Ces procédures qualifiées d'*Alternative Dispute Resolution Mechanisms (ADR)* ou, en français, de résolution extrajudiciaires des litiges (REL) peuvent être gérées de manière électronique : elles portent alors le nom d'*Online Dispute Resolution Mechanisms (ODR)*. Ces ADR ou ODR peuvent être développées par des organismes privés comme TRUST-e ou BB on Line, organismes installés aux États-Unis ou en Europe comme Trusted Shops ou faire l'objet d'une mise en place par les pouvoirs publics, comme le certificat *Privacy Mark* japonais[31]. Dans tous les cas, il s'agit d'assurer un accès à des moyens

[31] Mis en place dès 1998 par une coopération entre le MITI et l'association des entreprises et conduite par le *Japan Information Processing Development Cooperation* (JIPDEC). Sur ce système, voy. le site http://privacymark.org/index.html. Pour un tableau d'ensemble et

simples, efficaces, rapides et peu onéreux de résoudre les litiges nationaux et transfrontaliers résultant de la vente de marchandises ou de la prestation de services. Ces procédures devraient profiter aux consommateurs et donc renforcer leur confiance dans le marché. L'accès devrait valoir aussi bien pour les transactions en ligne que pour les transactions hors ligne et revêt une importance particulière lorsque les consommateurs font des achats dans un autre pays.

Ces mécanismes déjà reconnus et promus par l'article 17 de la directive sur certains aspects du commerce électronique ont depuis fait l'objet d'une directive spécifique[32]. On note cependant que la première directive avait circonscrit son champ d'application aux seuls litiges « entre des consommateurs et des professionnels concernant les obligations contractuelles découlant des contrats de vente ou de service, tant en ligne que hors ligne, dans tous les secteurs économiques, … ». Or, la référence de l'article 40 du Règlement à l'existence de modes de résolution de litiges extrajudiciaires suggère que demain les ODR et ADR pourront également s'occuper des litiges en matière de protection des données à caractère personnel même en dehors de transactions commerciales, ainsi pouvoir concerner des litiges employeurs-employés ou s'appliquer en matière de santé voire dans les relations entre les administrations et les citoyens.

11. Cette réserve faite, on suppose que nombre de dispositions de la directive relative aux ADR ou ODR présentes dans le cadre de transactions économiques 'consommateurs entreprises' s'appliqueront aux plateformes de règlement des litiges mises en place en matière de protection des données. Ceci apparaît évident dans les cas où, mises en place pour des litiges entre consommateurs et entreprises, les plateformes auraient également une compétence pour les litiges entre consommateurs et entreprises concernant les questions de protection des données. La solution devrait, me semble-t-il, être la même pour des plateformes s'occupant exclusivement de protection des données quel que soit le champ d'activités couvert, du moins en ce qui concerne les dispositions relatives aux conditions relatives à l'infrastructure mise en place[33], les dispositions

comparatif des labels 'privacy', lire R. Rowena, D. Wright, K. Wadhwa, « Developing a Privacy Seal », *International Data Privacy Law,* 2013, vol. 3, n° 2, pp. 100 et s.

[32] Directive 2013/11/UE du Parlement européen et du Conseil du 21 mai 2013 relative au règlement extrajudiciaire des litiges de consommation et modifiant le règlement (CE) 2006/2004 et la directive 2009/22/CE, *J.O.,* L 165/63 du 21 mai 2013.

[33] Art. 5.2 de la Directive : « Les États membres veillent à ce que les entités de REL :

a) tiennent à jour un site internet qui fournisse aux parties un accès aisé aux informations concernant la procédure de REL et qui permette aux consommateurs d'introduire une plainte et de soumettre les justificatifs nécessaires en ligne ;

relatives à la compétence et à l'indépendance des « juridictions »[34], à la parité des membres des juridictions, les uns représentant les responsables de traitement, les autres, les personnes concernées, à la transparence de la composition, du fonctionnement et des résultats d'activité, aux exigences d'équité (par exemple, le droit de se retirer de la procédure extrajudiciaire) et de légalité des décisions (non contradiction avec la loi). On notera que le règlement spécifie comme la directive ADR que le recours à une telle plateforme de règlement des litiges se fait « sans préjudice des droits des personnes concernées au titre des articles 77 et 79 ». En d'autres termes, le fait d'avoir accepté un code de conduite qui entraîne l'acceptation de se soumettre à un mécanisme de règlement extrajudiciaire ne peut avoir pour effet de priver la personne concernée du droit de recourir aux procédures devant l'autorité de contrôle et *a fortiori* devant la juridiction officielle[35].

---

b) fournissent aux parties, si elles en font la demande, les informations visées au point a) sur un support durable ;

c) le cas échéant, permettent au consommateur d'introduire une plainte hors ligne ;

d) permettent l'échange d'informations entre les parties par voie électronique ou, s'il y a lieu, par voie postale ;

e) traitent à la fois les litiges nationaux et les litiges transfrontaliers, et notamment les litiges relevant du règlement (UE) no 524/2013 ;

et f) prennent les mesures nécessaires, quand elles traitent des litiges relevant de la présente directive, pour garantir que le traitement des données à caractère personnel respecte les règles de protection des données à caractère personnel établies par la législation nationale transposant la directive 95/46/CE dans l'État membre dans lequel l'entité de REL est établie ».

[34] En particulier, l'article 26.1 : « Les États membres veillent à ce que les personnes physiques chargées du REL aient les compétences nécessaires et soient indépendantes et impartiales. Ils s'assurent à cet effet que ces personnes :

a) possèdent les connaissances et les aptitudes nécessaires dans le domaine du règlement extrajudiciaire ou judiciaire des litiges de consommation (en l'occurrence, ici, en matière de protection des données), ainsi que d'une compréhension générale du droit ;

b) soient nommées pour une durée suffisante pour assurer l'indépendance de leurs actions et qu'elles ne soient pas susceptibles d'être relevées de leurs fonctions sans juste motif ;

c) ne reçoivent pas d'instructions de l'une des parties ou des représentants de celles-ci ;

d) soient rémunérées d'une façon qui n'a pas de rapport avec le résultat de la procédure ;

e) communiquent sans tarder à l'entité de REL toute circonstance susceptible d'affecter ou d'être considérée comme affectant leur indépendance et leur impartialité ou de donner lieu à un conflit d'intérêts avec l'une ou l'autre partie au litige qu'elles sont chargées de résoudre. L'obligation de communiquer ces circonstances est une obligation permanente tout au long de la procédure de REL. Elle n'est pas applicable lorsque l'entité de REL n'est composée que d'une personne physique ».

[35] Ce point est rappelé à l'article 79, alinéa 1, du RGPD : « Sans préjudice de tout recours administratif ou extrajudiciaire qui lui est ouvert, y compris le droit d'introduire une réclamation auprès d'une autorité de contrôle au titre de l'article 77, chaque personne concernée a

CHAPITRE 2. Les balises mises par le Règlement

12. Cette confiance est cependant entourée de balises et d'exigences soulignées en particulier récemment par le Groupe 29 lors de son examen d'un projet de code de conduite en santé mobile[36]. Lors de cet examen[37], le Groupe 29 prend soin de souligner qu'un code de conduite n'a de valeur qu'à la triple condition suivante. Premièrement, les engagements qu'il contient doivent être clairs[38]. Deuxièmement, ils doivent être conformes aux exigences du Règlement et des législations (au sens le plus large) européennes et nationales applicables[39]. Troisièmement et surtout, ils doivent apporter par leur contenu spécifique une plus-value au regard de problématiques et questions spécifiques rencontrées par les organisations auxquelles le code est censé apporter des réponses claires et opérationnelles.

13. Les deux dernières conditions sont reprises par le Règlement. En ce qui concerne la conformité, l'article 40.1 du RGPD insiste sur le fait que les codes de conduite sont « destinés à contribuer à la bonne application du présent Règlement, compte tenu de la spécificité des différents secteurs de traitement et des besoins spécifiques des micro, petites et moyennes entreprises ». L'article 42, de manière parallèle, encourage les certifications et labels souscrits « aux fins de démontrer que les opérations de traitement effectuées par les responsables du traitement et les sous-traitants respectent le présent règlement ». En ce qui concerne la plus-value, elle peut ressortir

droit à un recours juridictionnel effectif si elle considère que les droits que lui confère le présent règlement ont été violés du fait d'un traitement de ses données à caractère personnel effectué en violation du présent règlement ».

[36] À l'occasion de sa lettre du 10 avril 2017 (disponible sur le site du Groupe 29 : *ec.europa.eu/justice/data-protection/article-29.*), adressée à l'éditeur du projet de code de conduite « Privacy en santé mobile », le Groupe 29 a délivré ses commentaires relatifs à la conformité des codes de conduite au regard des exigences posées par la directive de protection des données de 1995 et du RGPD, en dégageant un certain nombre de principes fondamentaux et généraux relatifs à leur élaboration. En particulier, le groupe rappelle la nécessité de valeur ajoutée que doit apporter le code de conduite.

[37] Sur ce cas, lire l'excellent commentaire de M. Brac de La Perriere et B.V. Labyod, « Code de conduite européen « Privacy en santé mobile », *Alain-Bensoussan.com*, 02 mai 2017, disponible à l'adresse : https://www.alain-bensoussan.com/avocats/rgpd-et-codes-de-conduite-g29/2017/06.

[38] On rappelle les critiques émises à ce propos par J. Reidenberg *et al.*, dans l'article cité *supra*, note 19.

[39] En l'occurrence, le projet de code de conduite m-santé, selon le Groupe 29, aurait dû prendre en compte d'autres éléments de la règlementation qui impactent la conformité en matière de protection des données, comme la « directive ePrivacy » s'agissant de la mise en œuvre des cookies, le règlement « eIDAS » (en matière d'identification électronique et de services de confiance), ou la directive 93/42/CE relative aux dispositifs médicaux.

de son contenu par les précisions apportées par le code de conduite, de la procédure d'adoption du code qui garantit l'engagement des auteurs du code, des modes particuliers d'information tant des personnes concernées que des employés du responsable du traitement, et enfin de la référence dans le code à l'existence de mécanismes d'audit et d'approbation par des organismes de contrôle ou de certification compétents en ce qui concerne tant les codes de conduite que les certifications et labels[40].

Ces exigences de plus-value, de transparence et de conformité ne sont pas sans rappeler les principes établis par le défunt Accord interinstitutionnel conclu entre Parlement européen, Conseil et Commission européenne le 16 décembre 2003[41] à l'acceptation de modes de régulation alternatifs que cet Accord reconnaît utiles[42] : « La Commission, affirme le point 17

[40] En ce qui concerne les certifications ou labels, le RGPD prévoit (art. 42) qu'ils ne pourront être délivrés que par un organisme de certification disposant d'un niveau d'expertise approprié en matière de protection des données ou par l'autorité de contrôle compétente sur la base de critères approuvés par cette autorité de contrôle ou par le comité européen de la protection des données après transmission à ces organismes, par le responsable de traitements ou le sous-traitant, de toutes les informations relatives au traitement et communication d'un accès à ses activités de traitement. La délivrance de l'agrément est adressée pour une durée maximale de trois années.

[41] *J.O.*, C 321 du 31 décembre 2003, pp. 1 et s., disponible à l'adresse suivante : http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A32003Q1231%2801%29. Cet accord a été abrogé par un nouvel accord du même nom, approuvé le 13 avril 2016 : Accord interinstitutionnel entre le Parlement européen, le Conseil de l'Union européenne et la Commission européenne « Mieux légiférer » disponible à l'adresse suivante : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016Q0512%2801%29.

Il est à noter que les articles relatifs aux modes alternatifs ne sont pas repris dans ce nouvel accord qui se restreint à l'analyse des compétences des autorités européennes. Ce point est d'autant plus dommageable qu'à propos d'une autre innovation technologique, les robots, le Parlement européen (« Résolution du Parlement européen du 16 février 2017 contenant des recommandations à la Commission européenne concernant des règles de droit civil sur la robotique, 2015/2103 (INL), PA TA-PROV(2017) 0051) prône l'adoption de modes de régulation alternatives pour réguler outre la loi l'innovation technologique : « *The need to intervene timely, before the technology spreads, generates needs and users behaviors, thus triggers a market –demand, requires regulators to employ other instruments than old-style law. In this vein, the EU Resolution resorts quite heavily to soft law, in the form of codes of conduct for researchers, designers, users….* » (E. PALMERINI, « Towards a Robotics Law at the EU Level ? », in *L'intelligence artificielle et le droit* (H. JACQUEMIN et A. DE STREEL eds), Cahier du CRIDS, n° 41, Bruxelles, Larcier, 2017, p. 51).

[42] *Cf.* le point 16 de cet accord : « Les trois institutions rappellent que la Communauté ne légifère que dans la mesure nécessaire, conformément au protocole sur l'application des principes de subsidiarité et de proportionnalité. Elles reconnaissent l'utilité de recourir, dans les cas appropriés, lorsque le traité CE n'impose pas spécifiquement le recours à un instrument juridique, à des mécanismes de régulation alternatifs ». Le point 17 ajoute que « Ils (ces mécanismes) doivent assurer une régulation rapide et flexible qui n'affecte pas les principes de concurrence ni l'unicité du marché intérieur ».

de l'Accord, veille à ce que le recours aux mécanismes de corégulation et d'autorégulation soit toujours conforme au droit communautaire et qu'il respecte des critères de transparence (publicité des accords, accessibilité et lisibilité des formulaires notamment) et de représentativité des parties impliquées. Il doit en outre représenter une valeur ajoutée pour l'intérêt général… ». On note cependant qu'un critère pourtant proposé par l'Accord n'est pas repris par le texte du règlement : celui de la représentativité des parties concernées[43]. Il eût sans doute été bon que, comme l'Union européenne l'a fait en matière de commerce électronique, le RGPD spécifie que si possible, les codes de conduite soient rédigés avec ou après concertation avec les représentants des personnes concernées[44]. Ainsi, si

[43] *Cf.* toutefois, le considérant n° 99 du RGPD qui demande dans toute la mesure du possible qu'une consultation des personnes concernées ait lieu en cas de rédaction des codes de conduite. De manière plus générale, à propos des trois critères définis par l'Accord en ce qui concerne la recevabilité des modes de régulation alternatifs, lire nos réflexions Y. POULLET, « How to regulate Internet ? : New Paradigms for Internet Governance », in *Variations sur le droit de la société de l'information* (J. BERLEUR *et al.* ed.) coll. Cahiers du CRID, n° 20, pp. 130 et s). « *These three criteria are defined as follows :*

„- The „legitimacy" is „source oriented and underlines the question of the authors of a norm. To what extent, might the legal system accept a norm elaborated outside of the actors designated by the Constitution or under constitutional rules ? This quality of the norm means that the authorities in charge of the norm promulgation must be habilitated for doing that by the community or communities of the persons which will have to respect the rule they have enacted. This legitimacy is obvious as regards the traditional State authorities acting in conformity with the competence devoted to them by the Constitution. It is less obvious when the regulation is the expression of private actors themselves as it is the case with self-regulation, particularly when it is the fact of certain obscure associations or even of private companies able to impose their technical standards.

- The „conformity" is „content oriented" and designates the compliance of normative content vis-à- vis fundamental society values, those embedded undoubtedly in the legal texts but also beyond that those considered as ethical values to be taken into account by the legal system. Again this criterion is quite easy to satisfy and to verify in case of traditional texts issued by governmental authorities insofar these texts must be taken in consideration of already existing rules with superior values. It seems more intricate to satisfy to this criterion when the compliance with existing legislative text is not systematically checked insofar these texts are not existing or not clearly identified. Indeed self-regulation is often a way to avoid the traditional and constitutionally foreseen regulatory methods of rule-making.

- Finally, the „effectiveness" is „respect oriented". To what extent, a norm will be effectively respected by those to whom the norm is addressed ? So, the question about the information about the existence of the norms, about the sanctions and the way by which they might be obtained are central for determining the effectiveness of a norm. By this criterion, one means in particular the fact for the addressees of the norm to be aware of the content of the norm but also for norms to foresee a cost for its non-respect by addressees who are so stimulated to follow the rule ».

[44] *Cf.* à cet égard, l'article 16.2 de la directive 2000/31/CE sur certains aspects du commerce électronique du 8 juin 2000 : « Les États membres et la Commission encouragent les associations ou les organisations représentant les consommateurs à participer à l'élaboration et à l'application des codes de conduite ayant des incidences sur leurs intérêts… ». À noter

on considère les trois critères mis en évidence par l'analyse de l'ancien Accord interinstitutionnel, à savoir la légitimité des acteurs, la conformité du contenu et l'effectivité des mesures prises, on peut proposer la liste suivante des points auxquels les rédacteurs devront être attentifs.

14. En ce qui concerne la légitimité du mécanisme de régulation, il s'agira de vérifier la source du texte et/ ou du mécanisme mis en place. En particulier, la représentativité des auteurs dans le secteur si le mécanisme est prévu au niveau sectoriel et la concertation ou consultation des personnes concernées à travers les associations qui peuvent les représenter (par exemple : les syndicats pour un code de conduite sur la surveillance des employés, les consommateurs pour un code de conduite ou un certificat en support de transactions commerciales). On sera par ailleurs attentif à la publicité donnée au mécanisme tant en interne pour le personnel chargé au sein de l'organisation du responsable du traitement d'appliquer le mécanisme qu'en externe pour que les personnes concernées puissent aisément s'y référer. Vis-à-vis de ces destinataires, on veillera à ce que le langage soit clair, précis et compréhensible eu égard au type de public visé.

La conformité exige tout d'abord une bonne identification de l'ensemble des textes de protection des données applicables et ce, au sens le plus large, ainsi on devra tenir compte non seulement des textes législatifs ayant directement trait à la protection des données mais également de textes législatifs ou non ayant un impact en la matière comme des textes en matière de secret professionnel, des normes techniques ou réglementaires en matière de sécurité des données.

L'effectivité se mesure à différents critères : les uns portent sur le degré de connaissance interne et externe du mécanisme mis en place et les mesures organisationnelles et techniques prises pour faciliter cette connaissance ; d'autres porteront sur la possibilité plus ou moins aisée de mettre en œuvre les mécanismes mis en place : l'existence d'une adresse

---

cependant le considérant n° 99 du RGPD : « Lors de l'élaboration d'un code de conduite, ou lors de sa modification ou prorogation, les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants devraient consulter les parties intéressées, y compris les personnes concernées lorsque cela est possible, et tenir compte des contributions transmises et des opinions exprimées à la suite de ces consultations ». Cette réflexion rejoint la volonté exprimée par le gouvernement Obama en 2012 qui réclamait un « *open transparent forum in which stakeholders who share an interest in specific market or business contexts will work toward consensus on appropriate, legally enforceable codes of conduct* » (The White House, *Consumer Data Privacy in a Networked World : A framework for Protecting Privacy and Promoting Innovation in the Global Digital World,* février 2012, disponible à *http://www.white-house.gov/sites/default/files/privacy-final.pdf*).

de contact, le degré de rapidité de réaction, l'existence de formulaires de plainte, etc. ; d'autres encore portent sur les mesures mises en place en interne (par exemple : training du personnel, consignes de sécurité,…) ou en externe (par exemple les audits) pour favoriser l'application effective des dispositions du code de conduite et le contrôle de cette application ; d'autres portent sur la possibilité d'introduire des suggestions d'amélioration ou des plaintes en matière de non-respect des mécanismes mis en place voire des procédures indiquées et, dans ce dernier cas, les qualités d'efficacité, d'indépendance des personnes appelées à examiner les litiges ; d'autres, enfin, sur l'adéquation et le caractère approprié des sanctions et autres mesures mises en place pour assurer la satisfaction des personnes concernées et la couverture de leurs préjudices tant matériels que moraux.

15. Le contrôle des pouvoirs publics sur les mécanismes de régulation alternatifs, par ailleurs encouragés, existe non seulement lors de la création des instruments mais tout au long de leur vie. Ainsi, le suivi de la bonne application des codes de conduite est assuré par un « organisme qui dispose d'un niveau d'expertise approprié au regard de l'objet du code et qui est agréé[45] à cette fin par l'autorité de contrôle compétente »[46]. La suspension ou l'exclusion d'un responsable de traitement ou sous-traitant ayant violé le code peuvent être décidées par l'organisme en question[47], lui-même sous contrôle de l'autorité compétente. L'article 43 du RGPD prévoit de son côté que les organismes de certification doivent être agréés[48], moyennant le respect de certaines conditions d'expertise, d'indépendance et d'efficacité dans le travail. Ces organismes ou l'autorité de protection des données peuvent également décider de suspendre ou de révoquer une certification ou un label.

---

[45] L'article 41.2 fixe les conditions d'agréation par l'autorité de contrôle.

[46] Art. 41. 1.

[47] L'organisme agréé dispose alors de pouvoirs importants : « Sans préjudice des missions et des pouvoirs de l'autorité de contrôle compétente et des dispositions du chapitre VIII, un organisme visé au paragraphe 1 du présent article prend, sous réserve des garanties appropriées, des mesures appropriées en cas de violation du code par un responsable du traitement ou un sous-traitant, et peut notamment suspendre ou exclure le responsable du traitement ou le sous-traitant concerné de l'application du code. Il informe l'autorité de contrôle compétente de ces mesures et des raisons pour lesquelles elles ont été prises ».

[48] Art. 43.1 : « Les États membres veillent à ce que ces organismes de certification soient agréés par une des entités suivantes ou les deux :

a) l'autorité de contrôle qui est compétente en vertu de l'article 55 ou 56 ;

b) l'organisme national d'accréditation désigné conformément au règlement (CE) no 765/2008 du Parlement européen et du Conseil, conformément à la norme EN-ISO/IEC 17065/2012 et aux exigences supplémentaires établies par l'autorité de contrôle qui est compétente en vertu de l'article 55 ou 56 ».

On ajoute que l'agrément peut être retiré par celui qui l'a délivré.

L'approche européenne se caractérise donc par ce que l'Accord interinstitutionnel appelle une 'co-régulation'[49] et qu'il définit comme suit : « On entend par corégulation le mécanisme par lequel un acte législatif communautaire confère la réalisation des objectifs définis par l'autorité législative aux parties concernées reconnues dans le domaine (notamment les opérateurs économiques, les partenaires sociaux, les organisations non gouvernementales ou les associations). Un tel mécanisme peut être utilisé sur la base de critères définis dans l'acte législatif pour assurer l'adaptation de la législation aux problèmes et aux secteurs concernés, alléger le travail législatif en se concentrant sur les aspects essentiels, et profiter de l'expérience des parties concernées ».

16. Cette approche co-régulatrice se rapproche de celle développée au Japon[50] mais s'oppose à l'approche auto-régulatrice des États Unis où sauf exceptions[51], les codes de conduite suppléent à l'absence d'instruments législatifs voire justifient cette absence de législation[52]. Nombre de

[49] Sur ce concept, Y. POULLET, « How to regulate the Internet : New paradigms for Internet Governance ? », in *E-Commerce Law and practice in Europe* (I. WALDEN et J. HÖRNLE ed.), Cambridge, Woodehead, Section 1, Chap. 2 ; Y. POULLET, « Technology and Law : From Challenge to Alliance », in *Information Quality Regulation : Foundations, Perspectives and Applications,* Baden-Baden, Nomos, 2004 ; Y. POULLET, « Comment réguler la protection des données ? – Réflexions sur l'internormativité », in *Liber Amicorum P. Delnoy,* Bruxelles, Larcier, 2005, pp. 1075-1097 ; Y. POULLET, « Technologies de l'Information et « co-régulation » : une nouvelle approche », in *Liber Amicorum M. Coipel,* Antwerpen, Kluwer, 2004, pp. 167- 188.

[50] Selon H. Miyashita (« A Tale of Two Privacies : Enforcing Privacy with Hard Power and Soft Power », in *Enforcing Privacy* (D. WRIGHT et P. DE HERT eds), Springer, 2016, pp. 105 et s. : « *The trustmark was formed as a kind of co-regulation operated by private organisations expressly authorised by the Government* ».

[51] Ainsi, les législations 'The Children's Online Privacy Protection Act' ; 'The Gramm-Leach-Bliley Act' en matière financière et de crédit et 'The Health Insurance Portability and Accountability Act'. Sur ces trois législations, la présentation proposée par WIKIPEDIA (https://en.wikipedia.org/wiki/Privacy_policy) : « *The Children's Online Privacy Protection Act (COPPA) affects websites that knowingly collect information about or targeted at children under the age of 13. Any such websites must post a privacy policy and adhere to enumerated information-sharing restriction. COPPA includes a "safe harbor" provision to promote Industry self-regulation (COPPA compliant Privacy Policy). The Gramm-Leach-Bliley Act requires institutions "significantly engaged in financial activities" give "clear, conspicuous, and accurate statements" of their information-sharing practices. The Act also restricts use and sharing of financial information. The Health Insurance Portability and Accountability Act (HIPAA) privacy rules requires notice in writing of the privacy practices of health care services, and this requirement also applies if the health service is electronic* ».

[52] Sur cette volonté des promoteurs des codes de conduite américains d'éviter une législation, lire l'article très critique de la situation américaine de R. GELLMAN et P. DIXON, « Failures of Privacy Self Regulation in the United States », in *Enforcing Privacy* (D. WRIGHT et P. DE HERT eds), Springer, 2016, pp. 53 et s. Les auteurs décrivent comment des initiatives

commentateurs attribuent à cette absence de législation, l'échec de l'approche auto-régulatrice américaine et dénoncent la légèreté des codes de conduite, l'ineffectivité voire le caractère éphémère des systèmes de certification mis en place comme BB on Line, Trust-e, Webtrust ou TrustGuard[53], et l'absence totale de contrôle et de sanctions. Comme l'affirmait, dès 1997, D. Mulligan du Center for Democracy and Technology[54] : « *We strongly believe that appropriate legislation can protect privacy and aid electronic commerce by creating a level policy and practice playing field and a viable benchmark for oversight, enforcement, and redress. To accomplish the goals of protecting privacy and aiding electronic commerce, we believe that Congress should enact legislation enabling the Federal Trade Commission to craft baselines for protecting privacy during commercial interactions* ».

Certaines statistiques sont par ailleurs éloquentes[55]. On cite l'analyse en 2008 du Cy Lab de la Carnegie Mellon University à propos de 33.000 sites web utilisant la plateforme *Privacy Preferences* proposée alors par P3P. Sur ces 33.000 sites, pas moins de 11.500 erreurs et, notamment, des entreprises certifiées par e-Trust. *L'Electronic Frontier Foundation* relève que nombre de prestataires importants comme Facebook, Google, Amazon ont impunément modifié le contenu de leurs « *Privacy policies* »[56]. *La Federal Trade Commission* dont le rôle est capital puisqu'elle a la compétence légale de sanctionner les '*False or Deceiptive Privacy Statements*' que peut recéler une « *Privacy Policy* » reconnaît elle-même[57] que le système fonctionne mal et que même dans le contexte des '*Safe Harbor Principles'*, son action est révélée inopérante[58]. La longueur des « *privacy policies » (dix minutes de lecture en moyenne)*, le fait que seuls trois pour cent des consommateurs

comme « *the Privacy Leadership Initiative* », « *the Online Privacy Alliance* » et plus récemment celles de la *Federal Trade Commission (FTC)* sont nées de la volonté des entreprises d'éviter toute intervention législative.

[53] Sur ces différents organismes de certification, voy. les sites : "Privacy Seals & Services by Trust Guard" ; www.trust-guard.com ; « Privacy Certification » ; www.etrust.org ; http://www.webtrust.org/.

[54] « Testimony of Deirdre Mulligan before the Senate Committee on Commerce, Science and Transportation Subcommittee on Communications – Center for Democracy & Technology », disponible à l'adresse : www.cdt.org

[55] À cet égard, nous avons repris pêle-mêle certaines des observations et références reprises dans les articles déjà cités de Wikipedia, de Reidenberg *et alii*, de R. Gellman et Dixon.

[56] E. Millis, « EFF tracking policy changes at Google, Facebook and others », *Cnet Digital News*, June 2009, Cnet.com.

[57] *Cf.* le rapport de 2012 « *Protecting Consumer Privacy in an Era of Rapid Change* », disponible à http://ftc.gov/osf/2012/03/120326privacy report.pdf. qui conclut : « *Self-regulation has not gone far enough* » et « *There has been little self-regulation* ».

[58] Sur ce point, les données commentées par C. Connelly et P. van Dijk, « Enforcement and reforms of the EU-US Safe Harbor Agreement », in *Enforcing Privacy* (D. Wright et P. De Hert eds), Springer, 2016, pp. 270 et s.

les lisent et que nombre de personnes leur accordent une portée qu'elles n'ont pas[59] ajoutent à ce que Gellman et Dixon appellent à raison la faillite de l'autorégulation américaine si elle n'est point appuyée ou s'appuie sur un acte réglementaire public[60].

17. Trois arguments en faveur de la co-régulation me semblent à cet égard décisifs : le premier est le manque de principes auxquels une pure autorégulation peut se référer. Sans doute, évoquera-t-on les 'lignes directrices de l'OCDE' mais celles-ci sont trop générales pour servir d'assise à une écriture qui tient compte des enjeux actuels du numérique (ex le *profiling*, l'existence d'acteurs nouveaux comme les producteurs de biens ou de services intermédiaires, les modes de collecte (les objets intelligents) et de stockage (le cloud) nouveaux, etc.). Le deuxième argument est l'ineffectivité des systèmes de contrôles et de sanctions mis en place. Sans doute, la démarche d'appel au marché est intéressante mais comment pour les entreprises, responsables de traitement, justifier le recours à des mécanismes coûteux lorsque le consommateur lui-même n'y accorde que peu d'importance et comment, dans un marché de la certification concurrentiel, rendre possible et crédible l'intervention et la sanction d'organismes de certification souvent simples associations *non profit* face à des responsables de traitement par ailleurs clients dont les moyens sont sans commune mesure avec ceux de ces organismes. Et c'est le troisième argument, la recherche par la personne concernée d'un avantage à court terme qui souvent justifie la demande d'une prestation de services sur le Net, explique que cette dernière esquive le détour par la lecture d'une '*privacy policy*' et/ou du site web des organes de certification et ce, au profit d'un accès quasi direct au service alléchant proposé par le responsable du traitement.

---

[59] Deux points relevés dans une étude de 2007 menée par l'University of California, Berkeley : 1. « *75 % of consumers think 'as long as a site has a privacy policy it means it won't share data with third parties', confusing the existence of a privacy policy with extensive privacy protection* » ; 2. « *when not presented with prominent privacy information…" consumers were "…likely to make purchases from the vendor with the lowest price, regardless of that site's privacy policies* ».

[60] À cet égard, les remarques de Reidenberg *et alii* qui notent que la qualité des 'privacy policies' imposées dans le cadre des trois législations citées ci-dessus est meilleure que celle des autres.

CHAPITRE 3. L'acceptation des modes alternatifs de régulation et les flux transfrontières

18. Dans le cadre des flux transfrontières, l'attitude européenne se veut pragmatique mais ferme. Le chapitre y consacré par le Règlement témoigne d'un durcissement des conditions d'acceptation de la notion de 'protection adéquate' déjà proposée par la directive 95/46, en particulier en soulignant le rôle essentiel de protection des autorités de protection des données. Ce durcissement est sans hésitation une conséquence de la décision *Schrems*[61], dans une affaire concernant Facebook. Cette décision considérait en effet que le niveau de protection offert par les États-Unis n'est pas satisfaisant, nonobstant la décision d'adéquation de la Commission européenne dite « *Safe Harbor* » du 26 juillet 2000, dans la mesure où cette décision ne prenait pas en compte les risques de violation de la vie privée suite aux activités de la National Security Agency des États-Unis.

Par ailleurs, l'attitude européenne doit tenir compte du caractère global de l'Internet et de l'impossibilité d'imposer des frontières à la circulation des données à caractère personnel vers des pays sans législation de protection des données ou ne disposant pas de législations équivalentes, et donc pragmatiquement se doit d'accepter en externe des mécanismes alternatifs.

En matière de flux transfrontières, les articles 44 et suivants du Règlement reprennent l'essentiel du système proposé par les articles 25 et suivants de la directive 95/46 même si la formulation est plus positive, le Règlement ayant abandonné l'interdiction de principe au profit d'une formulation différente : « Un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale peut avoir lieu lorsque la Commission a constaté par voie de décision[62] que le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou l'organisation internationale en question assure un niveau de protection adéquat ». Ceci dit, l'évaluation du caractère adéquat renvoie désormais à des critères plus nombreux. Ainsi, en suivi de l'arrêt *Schrems*, « il est tenu compte de la législation pertinente, tant générale que sectorielle, **y compris** en ce qui concerne la sécurité publique, la défense, la sécurité nationale et le droit pénal ainsi que l'accès des autorités publiques aux données à caractère personnel, de même que la mise en

[61] C.J.U.E., 6 octobre 2015, arrêt *M. Schrems*, 362/14.

[62] Notons que ces décisions de la Commission doivent faire l'objet d'un avis préalable du Comité européen de protection des données et peuvent faire l'objet de recours par toute personne concernée devant la Cour de justice selon l'article 263 du TFUE.

œuvre de ladite législation », mais également de l'existence d'une autorité de contrôle indépendante disposant de pouvoirs d'action effectifs et enfin, d'engagements internationaux et la participation à des systèmes de protection des données multilatéraux (comme la référence aux principes directeurs de l'OCDE ou la ratification de la Convention 108 du Conseil de l'Europe sur la protection des données) ou régionaux comme *l'APEC Privacy Framework* adopté dans le cadre de l'accord de coopération économique entre pays du Sud Est Asie-Pacifique. Un document de travail adopté par le Groupe de l'article 29, le 6 février 2018[63], est particulièrement intéressant : il précise les exigences relatives au caractère adéquat tant du point de vue du contenu des règles, objet de l'examen d'adéquation, que du point de vue de leur effectivité. On relève en ce qui concerne le premier point que les principes de spécification des finalités, de durée limitée de conservation des données et de transparence des traitements ont été ajoutés ; en ce qui concerne le second point, figure le principe d'« *accountability* ».

19. À défaut de décision d'adéquation, le règlement réclame, comme le faisait la directive, des garanties appropriées de protection des données mais élargit la liste des moyens de leur obtention : ainsi aux clauses –types de protection des données adoptées par la Commission, l'article 46 ajoute les clauses-types adoptées par une autorité de contrôle et approuvées par la Commission, les codes de conduite ou mécanismes de certification approuvées par une autorité de contrôle et les 'règles de conduite contraignantes' existantes au sein d'un groupe multinational d'entreprises[64] dont le régime est détaillé à l'article 47.

Notre propos se limitera aux deux principales innovations : la première est la consécration par le règlement des 'règles d'entreprise contraignantes', création du groupe de l'article 29 et jusque-là sans fondement législatif ; la seconde concerne les modifications apportées à la reconnaissance européenne des codes de conduite made in US, dans le cadre du « *Privacy Shield* » (le 'bouclier européen en matière de protection des données') qui, suite à l'arrêt *Schrems*, a succédé au défunt '*Safe Harbor*',

[63] Ce document dit 'explicatif' fait suite à la proposition publiée pour avis et commentaires par le Groupe 29, le 29 novembre 2017. Ce document est publié sur le site du Groupe 29 (http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083).

[64] À cet égard, lire les documents explicatifs du Groupe 29 relatif au processus des transferts encadrés par des règles d'entreprise contraignantes : *Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules*, WP256 à destination des responsables de traitement et celui cette fois concernant les sous-traitants (WP257), disponible à http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

objet de la décision de la Commission le 26 juillet 2000[65], décision remise explicitement en cause par les juges de Luxembourg.

SECTION 1. – Les règles d'entreprise contraignantes

20. Reconnues dès 2007 de façon prudentielle par le Groupe 29[66], les règles d'entreprise contraignantes[1] (ou « BCR » pour *Binding Corporate Rules*) sont un instrument juridique européen auquel une société multinationale ou un groupe d'entreprises peut recourir afin de garantir un niveau adéquat de protection des données à caractère personnel lors du transfert de ces données, au sein du groupe, au départ d'un pays situé dans l'Union européenne (UE) ou dans l'Espace économique européen (EEE) vers un pays tiers.

Cette consécration législative va de pair avec des balises supplémentaires mises à ce mécanisme alternatif que sont les règles d'entreprise. Ainsi, le Règlement précise d'emblée que les règles d'entreprise ne pourront être validées qu'à la triple condition premièrement, qu'elles aient suivi la procédure de cohérence des articles 63 et suivants, qui soumettent le projet de règles à l'avis du Comité européen de protection des données, deuxièmement qu'elles soient juridiquement contraignantes pour les entreprises de même, ajoute le Règlement, que pour leurs employés[67] et enfin,

---

[65] Décision 2000/520/CE relative à la pertinence de la protection assurée par les principes de la sphère de sécurité et par les questions souvent posées y afférentes publiées par le ministère du commerce des États-Unis d'Amérique, *J.O.C.E.,* 25 août 2000, I, 215, pp. 7 à 47.

[66] Voilà la liste des Working Papers du Groupe 29 relatifs aux règles d'entreprise :

- WP 107 : Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules" ;
- WP 108 : Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules ;
- WP 133 : Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data ;
- WP 153 : Working Document setting a table with the elements and principles to be found in Binding Corporate Rules ;
- WP 154 : Working Document Setting up a framework for the structure of Binding Corporate Rules ;
- WP 155 : Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules.

[67] Le 6 février 2018, le groupe de l'article 29 a adopté deux documents de travail fixant les éléments et principes qui doivent se retrouver dans le règles d'entreprise contraignantes en distinguant les exigences posées aux responsables de traitement, d'une part et aux sous-traitants, d'autre part. Ces documents font suite aux propositions publiées pour avis et commentaires par le Groupe 29 le 29 novembre 2017. Ces documents sont publiés sur le site du Groupe 29 (http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083). Ces deux

troisièmement, que sur cette base, les personnes concernées jouissent de droits opposables devant les tribunaux[68]. L'article 49.2 décrit le contenu minimum de tout projet de règles contraignantes et ne se contente pas d'introduire les nouveautés explicites du règlement comme l'exigence d'un délégué, des engagements en ce qui concerne le profilage, etc. On note en particulier que le principe de la responsabilité des entités présentes sur le territoire européen est affirmé pour toute violation du règlement, peu importe la localisation du membre du groupe d'entreprises[69], et que des mécanismes d'audit et de réception des plaintes doivent exister dans le groupe d'entreprises[70]. Les codes de conduite acceptés avant l'entrée en vigueur du règlement restent valables, sauf à l'autorité de contrôle de les déclarer insuffisants. Toute modification d'un règlement d'entreprise doit être portée à la connaissance de l'autorité de protection leader. On conclut en soulignant que, comme pour les codes de conduite et les mécanismes de certification (*supra*, n^os^ 5 et s.), délégation est donnée à la commission pour préciser la forme de l'échange d'informations entre les responsables du traitement, les sous-traitants et les autorités de contrôle, ainsi que les procédures qui s'y rapportent.

---

documents prennent soin de fixer les règles transitoires et interprètent la notion de garanties appropriées reprise au texte des articles 47 et s., notamment en distinguant ce qui doit être partie intégrante des règles telles qu'elles devront être publiées et ce qui doit accompagner la demande introduite auprès des autorités de contrôle. On note en particulier l'ajout de dispositions relatives à la transparence et l'engagement de voir les recours fixés sur le territoire de l'Union européenne, lorsqu'un membre du groupe d'entreprises est situé en Europe. Les deux documents ont été finalement approuvées le 18 avril 2018 : « Recommendation on the approval of the Controller Binding Corporate Rules form (wp264) » et « Recommendation on the approval of the Processor Binding Corporate Rules form (wp265) », disponible sur le site du Groupe 29 : http://ec.europa.eu/newsroom/article 29/item-detail.cfm?item_id=623848.

[68] Les recommandations citées note précédente précisent que les engagements contenus dans les règles dites 'contraignantes' nées de l'adoption par le Groupe d'entreprise doivent générer des droits opposables devant les juridictions des pays des personnes concernées. Il revient par ailleurs au groupe de démontrer que les personnes concernées pourront, en vertu d'une sorte de « stipulation pour autrui », bénéficier de l'engagement pris envers l'autorité de contrôle.

[69] Art. 47, 2., f) : « l'acceptation, par le responsable du traitement ou le sous-traitant établi sur le territoire d'un État membre de sa responsabilité pour toute violation des règles d'entreprise contraignantes par toute entité concernée non établie dans l'Union ; le responsable du traitement ou le sous-traitant ne peut être exonéré, en tout ou en partie, de cette responsabilité que s'il prouve que le fait générateur du dommage n'est pas imputable à l'entité en cause ».

[70] Art. 47, j) : « les mécanismes mis en place au sein du groupe d'entreprises, ou du groupe d'entreprises engagées dans une activité économique conjointe pour garantir que [sic] le contrôle du respect des règles d'entreprise contraignantes. Ces mécanismes prévoient des audits sur la protection des données et des méthodes assurant que des mesures correctrices seront prises pour protéger les droits de la personne concernée. Les résultats de ce contrôle devraient être communiqués [au délégué à la protection des données et à l'autorité de contrôle] ».

SECTION 2. – Les mécanismes alternatifs dans le cadre du « Privacy Shield »

21. La CNIL[71] présente comme suit le « *Privacy Shield* » ou « Bouclier de protection des données » : « Le Bouclier de Protection des Données, mieux connu sous le nom de « Privacy Shield », est un mécanisme d'auto-certification pour les entreprises établies aux États-Unis qui a été reconnu par la Commission européenne comme offrant un niveau de protection adéquat aux données à caractère personnel transférées par une entité européenne vers des entreprises établies aux États-Unis. Ce mécanisme est par conséquent considéré comme offrant des garanties juridiques pour de tels transferts de données ». La décision européenne de remplacer la décision de 2000 dite « *Safe Harbor Principles* », prise après des négociations difficiles avec les États-Unis entamées dès le printemps 2015, s'expliquait non seulement par la délicate question du droit des autorités publiques américaines d'opérer des surveillances de masse auprès des responsables de traitement, ce qui entraîna le recours victorieux de Schrems auprès de la Cour de Luxembourg[72], mais également par les faiblesses du système d'autorégulation mis en place aux États-Unis et son manque d'effectivité[73].

22. Sur ce dernier point, une étude[74] sur les 1.597 organisations mentionnées sur le site du *Department of Commerce* américain, garant de

[71] Voy. le site : https://www.privacyshield.gov/Program-Overview. Le texte est présenté comme suit sur le site : « *The Privacy Shield program, which is administered by the International Trade Administration (ITA) within the U.S. Department of Commerce, enables U.S.-based organizations to join one or both of the Privacy Shield Frameworks in order to benefit from the adequacy determinations. To join either Privacy Shield Framework, a U.S.-based organization will be required to self-certify to the Department of Commerce (via this website) and publicly commit to comply with the Framework's requirements. While joining the Privacy Shield is voluntary, once an eligible organization makes the public commitment to comply with the Framework's requirements, the commitment will become enforceable under U.S. law. All organizations interested in self-certifying to the EU-U.S. Privacy Shield Framework or Swiss-U.S. Privacy Shield Framework should review the requirements in their entirety* ».

[72] Nous n'aborderons pas ici cette question ni la qualité des solutions offertes par le Privacy Shield à ce problème délicat de la surveillance de masse (création d'un ombusdman, possibilité d'intervention des Data Protection Authorities, etc.) Voy. sur cette question C. DE TERWANGNE et C. GAYREL, « Flux transfrontières de données et exigence de protection adéquate à l'épreuve de la surveillance de masse. Les impacts de l'arrêt Schrems », *Cah. dr. eur.*, 2018, pp. 35-81.

[73] *Cf.* le rapport de la Commission européenne soumis au Parlement en novembre 2013 : *Communication from the Commission to European Parliament and Council on the functioning of the Safe Harbor from the Perspective of European Citizens Established in the EU,* COM (2013), 847 final, Bruxelles, 27 novembre 2013.

[74] C. CONNOLLY, *Safe Harbor : Fact or Fiction*, disponible sur le site : http://Galaxia.com/public/research/assets/studies/safe_harbor_Fact_or_fiction_2008/ptrint-index.html.

l'application des '*Safe Harbor Principles*', ne mentionnait pas 206 entreprises qui pourtant affirmaient sur leur site être parties prenantes du *Safe Harbor*. D'autres affirmaient être couverts par un certificat sans que cela soit la réalité ; d'autres encore malgré leur violation des principes du Safe Harbor n'avaient jamais été inquiétées par la FTC, malgré les plaintes portées contre elles. Pas moins de 13 recommandations émises par la Commission en 2013 portaient sur le besoin d'adaptations majeures du système du *Safe Harbor* : manque de vérification et d'audits des entreprises pourtant certifiées, absence de publication des 'privacy policies', manque d'information et de collaboration avec les autorités européennes de protection des données, pas de lien automatique entre les '*privacy policies*' et le registre du Safe Harbor tenu par le *Department of Commerce*, coûts excessifs des procédures privées de règlement des litiges en particulier le *Judicial Arbitration Mediation Service (JAMS)*[75].

23. Le *Privacy Shield*[76] entend remédier à ces imperfections[77] même s'il respecte la différence d'approche américaine principalement d'autorégulation et l'approche européenne principalement legislative : « *While the United States and the European Union share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the European Union. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self-regulation* »[78].

Nonobstant ce rappel d'une distinction fondamentale quant au mode de régulation, le *Privacy Shield* affirme, comme le faisait déjà le *Safe Harbor* à propos de la Directive, les mêmes principes de base que le règlement européen : les entreprises européennes peuvent uniquement communiquer

[75] *Cf.* l'analyse du rapport et des défaillances du système américain, C. Conolly et P. van Dijk, « Enforcement and Reform of the EU-US Safe Harbor Agreement », in *Enforcing Privacy* (D. Wright et P. De Hert), Springer, 2016, pp. 261 et s.

[76] La décision de la Commission a été prise le 12 juillet 2016 et est en vigueur depuis le 1er août de cette même année. Sur cette décision et les documents y afférents, voy. le site de la CNIL : https://www.cnil.fr/fr/le-privacy-shield. Voy. égal. l'avis du Groupe 29 sur le projet déposé par la Commission en février 2016 et les critiques adressées à ce projet de texte : « *Although the WP29 does not expect the Privacy Shield to be a mere and exhaustive copy of the EU legal framework it considers that it should contain the substance of the fundamental principles and as a result, ensure an 'essentially equivalent 'level of protection* » (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf).

[77] Pour une analyse fouillée du *Privacy Shield* et de la protection adéquate ou non qu'il offre, voy. C. de Terwangne et C. Gayrel, « Flux transfrontières de données et exigence de protection adéquate à l'épreuve de la surveillance de masse. Les impacts de l'arrêt Schrems », *op. cit.*, pp. 53-73.

[78] Annexe 2 de la décision européenne, 12 juillet 2016, EU-U.S. PRIVACY SHIELD FRAMEWORK PRINCIPLES ISSUED BY THE U.S. DEPARTMENT OF COMMERCE disponible sur le site du *Privacy Shield*, https://www.privacyshield.gov/Program-Overview.

des données à caractère personnel à une société établie aux États-Unis si le transfert bénéficie d'une base de légitimité reconnue par le règlement. En outre, l'ensemble des autres obligations générales prévues par la législation européenne en matière de protection de données à caractère personnel pour le(s) transfert(s) doivent être respectées notamment, les principes de finalité, de proportionnalité y compris désormais de minimisation, de qualité des données. Les obligations d'information envers les personnes concernées, le droit d'accès et les droits d'opposition sont rappelés. Si les données ont vocation à être transférées à une société établie aux États-Unis, l'entreprise européenne qui transfère les données doit également informer les personnes concernées de l'identité des destinataires de leurs données et du fait que les données bénéficient de la protection accordée par le Bouclier de Protection des Données.

24. Quant au mécanisme d'engagement du respect des principes énumérés, proposé par le *Privacy Shield*, il reprend le mécanisme d'auto-certification déjà prévu par le Safe Harbor mais l'adapte quelque peu en tenant compte des critiques adressées par la Commission et la Cour de Justice. Le Département du commerce américain résume le mécanisme prévu comme suit : « *While decisions by organizations to thus enter the Privacy Shield are entirely voluntary, effective compliance is compulsory : organizations that self-certify to the Department and publicly declare their commitment to adhere to the Principles must comply fully with the Principles. In order to enter the Privacy Shield, an organization must (a) be subject to the investigatory and enforcement powers of the Federal Trade Commission (the "FTC"), the Department of Transportation or another statutory body that will effectively ensure compliance with the Principles (other U.S. statutory bodies recognized by the EU may be included as an annex in the future) ; (b) publicly declare its commitment to comply with the Principles ; (c) publicly disclose its privacy policies in line with these Principles ; and (d) fully implement them. An organization's failure to comply is enforceable under Section 5 of the Federal Trade Commission Act prohibiting unfair and deceptive acts in or affecting commerce (15 U.S.C. § 45(a)) or other laws or regulations prohibiting such acts* ». Sans doute, peut-on voir dans l'accord nouveau, un renforcement du contrôle *a priori* des engagements des organisations et entités lors de leur demande d'adhésion au Privacy Shield[79], en particulier, non seulement l'engagement du Department of Commerce américain de vérifier l'*accuracy*' du code de conduite des entreprises par rapport à la réalité, mais au-delà pour assurer le suivi de ces engagements, l'obligation d'introduire dans les codes de

[79] Sur cette demande d'adhésion, voy. le site https://www.privacyshield.gov/article?id=How-to-Join-Privacy-Shield-part-1.

conduite des mécanismes effectifs de recours et de sanctions[80], l'engagement du *Department of Commerce* d'entamer des investigations en cas de plaintes pour non-conformité[81], de même que la collaboration avec les autorités européennes de protection des données[82]. Par ailleurs, la liste des entreprises certifiées tenue par le *Department of Commerce* fera l'objet de révisions annuelles afin de veiller à sa fiabilité.

L'ensemble de ces précisions entend répondre aux lacunes décelées par la Commission européenne et rappelées ci-dessus. Elles témoignent de la volonté exprimée par l'Europe de ne plus se satisfaire du système d'autorégulation sans contrôle effectif des autorités publiques que le *Safe Harbor* avait mis en place. Ceci dit, il reste à s'interroger sur la façon dont l'administration américaine mettra effectivement en place ces nouveaux

---

[80] Voy. le texte de l'annexe II du Privacy Shield (pt 7) « *a. Effective privacy protection must include robust mechanisms for assuring compliance with the Principles, recourse for individuals who are affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum such mechanisms must include :*

i. readily available independent recourse mechanisms by which each individual's complaints and disputes are investigated and expeditiously resolved at no cost to the individual and by reference to the Principles, and damages awarded where the applicable law or private-sector initiatives so provide ;

ii. follow-up procedures for verifying that the attestations and assertions organizations make about their privacy practices are true and that privacy practices have been implemented as presented and, in particular, with regard to cases of noncompliance ; and

iii. obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.

b. Organizations and their selected independent recourse mechanisms will respond promptly to inquiries and requests by the Department for information relating to the Privacy Shield. All organizations must respond expeditiously to complaints regarding compliance with the Principles referred by EU Member State authorities through the Department. Organizations that have chosen to cooperate with DP As, including organizations that process human resources data, must respond directly to such authorities with regard to the investigation and resolution of complaints ».

[81] Voy. le texte de l'annexe II du "Privacy Shield" : « *When an organization becomes subject to an FTC or court order based on noncompliance, the organization shall make public any relevant Privacy Shield related sections of any compliance or assessment report submitted to the FTC, to the extent consistent with confidentiality requirements. The Department has established a dedicated point of contact for DP As for any problems of compliance by Privacy Shield organizations. The FTC will give priority consideration to referrals of non-compliance with the Principles from the Department and EU Member State authorities, and will exchange information regarding referrals with the referring state authorities on a timely basis, subject to existing confidentiality restrictions* ».

[82] Les organisations ou entités qui rejoignent le Privacy Shield « will cooperate with the DP As in the investigation and resolution of complaints brought under the *Privacy Shield ; and iii. will comply with any advice given by the DP As where the DP As take the view that the organization needs to take specific action to comply with the Privacy Shield Principles, including remedial or compensatory measures for the benefit of individuals affected by any non-compliance with the Principles, and will provide the DPAs with written confirmation that such action has been taken* ».

engagements[83]. Le rapport publié par la Commission moins d'un an après la mise en œuvre du « *Privacy Shield* »[84] est optimiste à cet égard : « *The certification process has been handled in an overall satisfactory manner and more than 2400 companies have been certified so far. The U.S. authorities have put in place the complaint-handling and enforcement mechanisms and procedures to safeguard individual rights. This includes also the new additional redress avenues for EU individuals such as the arbitration panel and the Ombudsperson mechanism. Regarding the latter, an Acting Ombudsperson was designated following the change of Administration in January 2017, whereas the nomination of a permanent Ombudsperson is pending. Cooperation with European data protection authorities has been stepped up* ». Sans doute, le rapport pointe encore dix améliorations souhaitables dans le fonctionnement du processus parmi lesquelles on relève que la publication des certificats des entreprises devra suivre et non précéder la révision qui sera opérée par le *Department of commerce*, suite à l'adoption des *Privacy Shields*. Le *Department of Commerce* est en outre appelé à prendre des mesures proactives de contrôle du respect des engagements des entreprises, à développer sa politique d'information sur les règles du *Privacy Shield* et sa coopération avec les autorités européennes. Enfin, la question des systèmes automatisés de décision et de l'adéquation de la protection offerte aux États-Unis devra, toujours selon le même rapport, être approfondie.

Sans doute, le rappel par la Cour de Justice de Luxembourg dans l'arrêt *Schrems* du devoir de nos autorités de protection des données de veiller au respect des engagements en matière de protection des données, de contrôler l'action de la Commission à cet égard et de ne pas hésiter à intenter des recours constitue une garantie supplémentaire de voir les progrès promis par le nouvel accord EU – US se réaliser effectivement.

Conclusions

25. Le nouveau règlement européen appelle à une meilleure prise en compte des mécanismes alternatifs de régulation et de règlement de conflits. Sa volonté de donner aux codes de conduite, aux mécanismes de

[83] À cet égard, le fait qu'avant même la décision de ratification des privacy Shields, la décision européenne soit déjà contestée. Sur ce point, lire : https://www.silicon.fr/privacy-shield-pas-ratifie-mais-attaque-152492.html#8rzDLvX5fohoRJ1p.99?inf_by=5a574cc7671db861688b458e.

[84] *Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU–U.S. Privacy Shield,* Bruxelles, 18 octobre 2017, COM (2017) 611 final.

certification et aux ADR la consécration législative, sa reconnaissance d'un véritable intérêt de ces mécanismes non seulement pour les promoteurs de ces codes mais également pour les personnes concernées et de leur associer des effets juridiques importants, en particulier le renversement de la charge de la preuve en cas de plaintes pour non-conformité aux exigences du règlement, doit être soulignée. Elle laisse augurer de l'éclosion de nombre de codes, certificats et plateformes de règlement de litiges qui, on le pressent, constitueront autant de garanties de la prise en charge par leurs promoteurs de la cause de la protection des données.

Dans le même temps, l'appel à ces mécanismes se fait dans la continuité des principes énoncés alors par l'Accord interinstitutionnel de 2003 'Bien légiférer' abandonné la veille de l'adoption du règlement, qu'il a pourtant inspiré. Cet accord tout en soulignant l'opportunité de ces mécanismes en balise très soigneusement la validité par un contrôle strict de conformité, de légitimité et d'effectivité. L'exigence de plus-value souligne que les mécanismes alternatifs ne peuvent être un substitut mais un complément à ce qui reste le pilier de la régulation, à savoir la réglementation législative. En matière de protection des données, il faut donc parler de co-régulation et pour être plus précis de co-régulation descendante dans la mesure où le recours au mécanisme suit l'intervention législative et est appelé par elle dans un cadre strict de contrôle par les autorités publiques. Ce n'est pas une co-régulation ascendante où l'autorégulation est première et réclamerait par la suite, afin de confirmer sa validité et ajouter à son effectivité, une demande de reconnaissance législative.

Ce souci de rendre effectif ce qui pourrait rester des principes certes généreux mais à usage purement rhétorique est manifestement une caractéristique du règlement. Au-delà de notre sujet, on souligne que les autorités de protection des données, à l'action désormais plus cohérente, voient leurs compétences et leurs moyens renforcés, que la technologie via les principes de *Privacy by design, privacy by default* et de réciprocité devient un allié de la législation européenne, que l'élargissement des droits de la personne concernée et la possibilité d'un recours collectif constituent autant de signes de cette volonté d'une meilleure effectivité. Pour revenir au sujet de notre réflexion, notons que l'effectivité est également recherchée via un renforcement de ce que Frison-Roche appelle le droit de la « c*ompliance* ». Ce droit s'exprime dans le règlement, tant en ce qui concerne les modes de régulation alternatifs étudiés : les codes de conduite, la certification, la labellisation, les ADR mais également, par l'exigence, dans les grandes entreprises ou à propos des traitements à hauts risques, de la nomination d'un délégué à la protection des données voire d'un *Privacy Impact Assessment*, par les règles d'entreprise contraignantes proposées aux multinationales comme condition d'offre de garanties adéquates. En

d'autres termes, c'est à l'intérieur des entreprises et, en tout cas, avec leur plein appui individuel et/ou collectif[85] qu'est recherchée cette effectivité. Appelés à être de '*good corporate citizens*'[86], les responsables de traitement deviennent les premiers agents du respect des prescrits. Comme l'écrit Frison-Roche[87], « dans le même temps que le droit de la compliance consiste à internaliser le droit de la régulation dans les entreprises en position de rendre mondialement effectif celui-ci, le droit de la compliance assure cette effectivité en contrôlant la mise en œuvre : il instaure en même temps la supervision de ces entreprises cruciales par les autorités de régulation. C'est ainsi qu'un nouveau continuum révolutionnaire s'est mis en place entre régulation, supervision, compliance ». Difficile de mieux exprimer l'apport décisif en la matière de notre Règlement.

Un dernier mot sur la question des flux transfrontières et la façon dont cette même effectivité de protection est recherchée. Si l'Europe ne peut imposer, à l'extérieur de ses frontières, sa conception de la co-régulation, elle se doit cependant, face à ce qui pourrait être une auto-régulation sauvage, d'exiger un minimum de respect des principes essentiels de protection des données en cas de flux transfrontières. C'est en tant que garante des libertés de ses citoyens, que se justifie l'exigence par l'Union européenne, d'une protection adéquate offerte par les destinataires hors frontières européennes. Là également, l'Europe à la fois étend sa reconnaissance de mécanismes alternatifs, en particulier par la reconnaissance des règles d'entreprises contraignantes mais, dans le même temps, limite sévèrement l'autorégulation par des balises renforcées du contenu de celles-ci mais surtout par l'exigence d'un contrôle des autorités publiques étrangères et la coopération avec les autorités de protection des données européennes, comme le montre l'étude du système du *Privacy Shield*.

[85] Ainsi par l'adoption de codes de conduite propres à une communauté ou association d'entreprises ou de mécanismes de labellisation ou de certification.

[86] L'expression est de B. DE JUVIGNY, « La compliance, bras armé de la regulation », in *Régulation, supervision et compliance* (M.A. FRISON-ROCHE dir.), Paris, Dalloz, 2017, p. 17.

[87] M.A. FRISON-ROCHE, « Du droit de la regulation au droit à la compliance », in *Régulation, supervision et compliance* (M.A. FRISON-ROCHE dir.), Paris, Dalloz, 2017, p. 17.